IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF THE PREMISES LOCATED AT 360 NARROWS ROAD, BARNSTEAD, NEW HAMPSHIRE 03225 AND THE PERSON OF CAROLINE ELLISON	)	No. 1:22-mj- 237-01-AJ
		FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A WARRANT

I, Kristin Allain, being duly sworn, depose and state that:

INTRODUCTION AND BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI" or "Investigating Agency"). As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I am currently assigned to an FBI squad that investigates white collar crimes. During the course of my duties, I have received training about and participated in the execution of search warrants, and the review and analysis of both physical and electronic evidence.

2. I submit this affidavit in support of an application to search and seize electronic devices belonging to Caroline Ellison (DOB: 11/1/1994) located (a) in the house located at 360 Narrows Road, Barnstead, New Hampshire 03225 (the "Subject Premises"), which is described in Attachment A-1, and (b) on the person of Caroline Ellison (the "Subject Person"), who is depicted in Attachment A-2.

3. As part of my duties, I am currently participating in an investigation into suspected criminal activity relating to FTX.com, FTX.us, and Alameda Research. I am familiar with the facts and circumstances of this investigation, and I have received information from a variety of sources, including but not limited to other law enforcement officers and agents, a confidential source of information, and my personal review of records relating to the investigation.

4. For the reasons detailed below, there is probable cause to believe that any electronic devices in the possession of Ellison or found within the Subject Premises contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1349 (wire fraud conspiracy); and 18 U.S.C. §§ 1956 and 1957 (money laundering and money spending) (the "Subject Offenses").

5. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

FACTS ESTABLISHING PROBABLE CAUSE

6. The U.S. Attorney's Office for the Southern District of New York and Federal Bureau of Investigation are investigating the possible misappropriation of billions of dollars in customer assets from the international cryptocurrency exchange FTX.com and its U.S. marketplace, FTX.us (hereinafter referred to together as "FTX") by certain corporate insiders

including Sam Bankman-Fried and Caroline Ellison, and the transfer of those misappropriated funds to a hedge fund owned by Bankman-Fried and managed by Ellison called Alameda Research ("Alameda"). As described below, there is probable cause to believe that Bankman-Fried, Ellison, and others known and unknown were involved in commission of the Subject Offenses, as described below.

Probable Cause Regarding the Subjects' Commission of the Subject Offenses

7. Based on my review of publicly available information, including news reports, public statements by Bankman-Fried, Ellison, and other employees of FTX and Alameda, documents produced by third parties, and other publicly available records, I have learned the following, in substance and in part:

a. FTX.com is a cryptocurrency exchange headquartered in the Bahamas that at its height had more than a million daily users and an average daily trading volume of approximately $10 billion or more. FTX.us is the United States affiliate of FTX.com. Both were founded by Bankman-Fried and were operating under his direction. As a cryptocurrency exchange, FTX accepted deposits of customer funds. Under FTX's terms of service, FTX stated that "none of the Digital Assets in [a customer's] Account are property of, or shall or may be loaned to, FTX Trading" and "At any time … [a customer] may withdraw [his or her] Digital Assets."

b. Alameda, which was principally owned by Bankman-Fried, was a quantitative trading firm specializing in cryptocurrencies. Alameda conducted cryptocurrency transactions through FTX. Caroline Ellison was the CEO of Alameda during the timeframe relevant to this investigation.

c. In or about May 2022, the crypto market experienced a crash resulting in a so-called "crypto winter," with many cryptocurrency businesses and cryptocurrencies collapsing in value.

In or around May and June of 2022, Alameda suffered a series of financial losses. Based on public reports and information provided by third parties, I understand that Alameda was also required to repay portions of large loans during that period. Subsequently, to address those financial issues, Bankman-Fried, with the assistance of others, including Ellison, secretly transferred billions of dollars from FTX to Alameda. The funds secretly transferred from FTX to Alameda included FTX customer deposits.

d. On or about November 2, 2022, the online publication Coindesk.com leaked a copy of Alameda's balance sheet (the "Coindesk Article"), which appeared to show that Alameda had approximately $14.6 billion in assets and $8 billion in liabilities, but that a large portion of the Alameda assets were either illiquid cryptocurrency or crypto tokens issued by FTX (called FTT).

e. Following publication of the Coindesk Article, on or about November 6, 2022, Changpeng Zhao, the co-founder and CEO of Binance, one of the largest cryptocurrency exchanges, tweeted in substance and in part: "As part of Binance's exit from FTX equity last year, Binance received roughly $2.1 billion USD equivalent in cash (BUSD and FTT). Due to recent revelations that have came [sic] to light, we have decided to liquidate any remaining FTT on our books." On or about November 6, 2022, following Zhao's tweet, the Twitter account @CarolineCapital, which appears to belong to Ellison, tweeted: "@cz_binance if you're looking to minimize the market impact on your FTT sales, Alameda will happily buy it all from you today at $22!"

f. Soon after Zhao's November 6, 2022 tweet, the value of the FTT token began falling and a high number of users of FTX sought to withdraw their assets from the platform, resulting in the equivalent of a cryptocurrency bank run of approximately $6 billion, the plummeting of FTT's value, and a liquidity crisis at FTX.

g. On or about November 7, 2022, Bankman-Fried tweeted, "A competitor is trying to go after us with false rumors. FTX is fine. Assets are fine." He added in a second tweet, in part, "FTX has enough to cover all client holdings. We don't invest client assets (even in treasuries). We have been processing all withdrawals, and will continue to be." In a third tweet, Bankman-Fried wrote, "It's heavily regulated, even when that slows us down. We have GAAP audits, with > $1B excess cash. We have a long history of safeguarding client assets, and that remains true today." Bankman-Fried subsequently deleted these tweets.

h. On or about November 10, 2022, it was publicly reported that FTX's liquidity crunch was in part due to undisclosed loans FTX had made to Alameda months earlier, after Alameda suffered a series of losses from deals. Those publications also reported that a portion of the loans from FTX to Alameda were made using FTX customer deposits, despite such use being prohibited by FTX's terms of service. On the same day, Bankman-Fried acknowledged the liquidity crunch at FTX.com, tweeting that he "fucked up." In the same Twitter thread, however, Bankman-Fried claimed that "FTX US USERS ARE FINE" and that FTX.us was "not financially impacted."

i. According to news reports, in a video meeting with Alameda employees on or about November 9, 2022, Ellison said, in substance and in part, that she, Bankman-Fried, and two other FTX executives, Nishad Singh and Gary Wang, had been aware of the decision to send customer funds from FTX to Alameda to help Alameda meet its liabilities.

j. According to news reports, Bankman-Fried secretly moved $10 billion in funds to trading firm Alameda, using a "backdoor" in FTX's book-keeping system, which was built using bespoke software, and allowed Bankman-Fried to execute commands that could alter the company's financial records without alerting other people, including external auditors, or raising

red flags.[1] Until recently, FTX employees were shown financial data that incorrectly suggested that even if all customers were to withdraw their funds, FTX would still have assets left over.

k. On or about November 11, 2022, the head of institutional sales at FTX acknowledged on Twitter that FTX had $8.8 billion in liabilities with only $900 million in liquid assets, and $5.2 billion in semi-liquid or illiquid assets, meaning FTX had a multi-billion dollar deficit. On or about November 12, 2022, a newspaper reported, based on a review of a balance sheet, that as of November 10, 2022, FTX held $900 million in liquid assets against $9 billion of liabilities.

l. On November 11, 2022, FTX.com, FTX.us, Alameda, and related entities all filed for bankruptcy. On the same day, Bankman-Fried resigned from the company.

8. Based on my conversations with another FBI Special Agent who participated in an interview with a former Alameda employee ("Employee-1"),[2] as well as my review of messages from the encrypted messaging application Signal, I have learned in substance and in part, that:

a. In connection with his work at Alameda, Employee-1 communicated with Ellison principally through Signal and Slack. Signal, as noted above, is an encrypted messaging application, but it may also be used to place encrypted voice calls. Slack is a messaging platform that may be used on a computer or through a phone. Slack messages can be sent to a single individual or a whole channel.

---

[1] In a text message to Reuters, Bankman-Fried denied implementing a "back-door," and claimed, in substance and in part, that his firm had "confusing internal labeling."

[2] Information from Employee-1 has been corroborated in part by other evidence, including Signal messages that have been produced by Employee-1 and notes that Employee-1 took prior to meeting with the FBI.

b. On or about November 2, 2022, Employee-1 communicated about the Coindesk Article with Bankman-Fried, Ellison, and one other Alameda employee using a group Signal chat. In the chat, Employee-1 asked whether "alameda's balance sheet leaked," and Bankman-Fried confirmed it had, and stated "don't know how."

c. On or about November 5 and 6, 2022, in the same Signal chat, Bankman-Fried, Ellison, and Employee-1 discussed how to respond to the decreasing price of FTT and Zhao's tweet that he was going to sell all of Binance's FTT. During that conversation, Ellison shared with the group her intention to tweet in response.

d. On or about November 6, 2022, in the same Signal chat, Bankman-Fried, Ellison, and Employee-1 discussed how Alameda could liquidate assets to assist FTX with covering customer withdrawals. During the same discussion, Ellison texted that one of Alameda's lenders was "asking what collateral we can post on a loan." Based on my involvement in this investigation, I understand that Ellison was referring to one of Alameda's lenders requesting that Alameda post additional collateral for its loan.

e. On or about November 7, 2022, on a Signal chat that included Bankman-Fried, Ellison, Employee-1, and other Alameda and FTX employees, Bankman-Fried asked, "1) how are withdrawals looking on FTX? 2) what's the ETA on getting ~$1b USD looking like?" In that same message thread, it appears that employees, including Ellison, were discussing liquidity issues with FTX US. As noted above, on the same day, Bankman-Fried tweeted, in part, "FTX is fine. Assets are fine."

f. Based on my review of Signal records and notes taken by Employee-1, I know that on November 7, 2022, Employee-1 called Ellison. During that call, Ellison informed Employee-1, in substance and in part, that FTX customer funds had been transferred to Alameda during an

Alameda credit crunch, resulting in a scenario where FTX would currently be a few billion dollars short if all FTX customers tried to withdraw their money.

g. Based on my review of Signal records and notes taken by Employee-1, I know that on or about November 9, 2022, Employee-1 was present by videoconference during the meeting at which Ellison stated that she, Bankman-Fried, Singh, and Wang were aware of the decision to send customer funds from FTX to Alameda.

9. Based on my review of documents and a recording provided by an investor in FTX, Bankman-Fried contacted potential investors on or about November 9, 2022—as FTX was experiencing a liquidity crunch—seeking a bailout of FTX. Among other things, Bankman-Fried provided potential investors a spreadsheet purporting to show FTX's assets and liabilities. Among FTX's liabilities, the document referred to a liability of $8 billion for a "Hidden, poorly internally labled [sic] 'fiat@' account," and $5 billion in "Withdrawals on Sunday," in apparent reference to the high-volume of customer withdrawals. The spreadsheet also included the following statement: "There were many things I wish I could do differently than I did, but the largest are represented by these two things: the poorly labeled internal bank-related account, and the size of customer withdrawals during a run on the bank."

10. Based on the foregoing, there is probable cause to believe that customer funds were misappropriated from FTX and transferred to Alameda, in breach of the representations made to customers in the terms of service, and that Ellison participated in, and was aware of the misappropriation of funds, in violation of the Subject Offenses.

Probable Cause Justifying the Search of the Subject Premises, Subject Person, and Electronic Devices Found Therein

11. For the reasons set forth below, there is probable cause to believe that the Subject Premises and the electronic devices in the possession of the Subject Persons will contain evidence,

fruits, and instrumentalities of the Subject Offenses. The applied-for warrant would authorize the search of (a) the Subject Premises as well as any closed containers or items contained therein and (b) the person of Caroline Ellison, and the seizure and forensic examination of any electronic device belonging to Ellison seized from her or the Subject Premises for the purpose of identifying electronically stored data or other evidence, fruits, or instrumentalities of the Subject Offenses, as particularly described in Attachment B. As described below, there is probable cause to believe that electronic devices are likely to be found on Ellison's person or in the Subject Premises, which is a home belonging to her parents, and that those electronic devices, including one or more cellphones and computers, were used as instrumentalities of and contain evidence of the Subject Offenses, as further described below.

12. First, there is probable cause to believe that Caroline Ellison is in possession of multiple electronic devices, and that those devices are likely to be found on her person or in Subject Premises, which is where she appears to be staying.

a. Based on my review of public sources, and my review of notes of an interview with Employee-1, I have learned that Ellison lived and worked in the Bahamas and Hong Kong. Additionally, I have learned from government records that on or about November 11, Ellison reentered the United States in Massachusetts and does not appear to have left the country.

b. On or about November 15, 2022, the Honorable Jennifer Willis, United States Magistrate Judge for the Southern District of New York, authorized a warrant and order for cellphone location information for a cellphone number that appears to belong to Ellison. The cellphone number is the number attributed to Ellison in Employee-1's cellphone. Based on cellphone location information provided by T-Mobile pursuant to the November 15, 2022, warrant and order, I have learned that the cellphone belonging to Ellison is in the vicinity of the Subject

Premises, including late at night and in the morning when Ellison would likely be sleeping. Accordingly, there is probable cause to believe that Ellison and her cellphone are likely to be found within the Subject Premises.

c. Based on my review public sources and database records available to the government, it appears that the Subject Premises is owned by Ellison's mother or both of her parents. Additionally, because it appears that Ellison traveled from a foreign country to the United States, it is likely that she brought electronic devices with her such as a personal laptop, tablet, additional cellphones, or other electronic devices related to cryptocurrency or financial information.

d. I know from my training and experience that when individuals are not home, they often take their cellphone(s) with them, and therefore if Ellison's cellphone is not in Subject Premises, it is likely to be on her person.

e. Accordingly, there is probable cause to believe that Ellison is currently staying at the Subject Premises and that her electronic devices, including but not limited to her cellphone, will be found on her person or in the Subject Premises.

13. Second, there is probable cause to believe Ellison's electronic devices will contain evidence and instrumentalities of the commission of the Subject Offenses. In particular:

a. As set forth above, there is probable cause to believe that Ellison used her cellphone to communicate with co-conspirators in the commission of the Subject Offenses. Specifically, it appears she used her cellphone to send Signal messages and also exchange telephone calls over Signal. For instance, as discussed above, Ellison used Signal on her cellphone to communicate with Bankman-Fried, Employee-1, and other employees about FTX's liquidity crisis, the sale of Alameda's assets, and her Twitter posts. Additionally, based on my review of publicly available

information about Signal, I have also learned that Signal has a computer application that allows the use of Signal over a computer. Accordingly, there is reason to believe that evidence of Signal communications will be found on Ellison's cellphone(s) or computer(s).

b. As set forth above, there is probable cause to believe that Ellison used her electronic devices to tweet on Twitter messages in furtherance of the Subject Offenses, including tweets about Alameda's balance sheet. Based on my review of Ellison's tweets, I know that her tweets were sent from the "Twitter Web App." According to publicly available information, the Twitter web application allows a user to access her or his Twitter account from any computer. Additionally, from my training and experience I know that individuals can tweet from their cellphones. Accordingly, there is probable cause to believe that Ellison's cellphone(s) or computer(s) will contain evidence of her Twitter activity.

c. Additionally, based on public information and information provided by Employee-1, I have learned that employees at Alameda and FTX used the application Slack to communicate amongst themselves. Slack is a messing service that can be accessed from a computer or cellphone. Accordingly, Ellison's electronic devices are likely to contain Slack communications.

d. Based on my training and experience, Ellison's electronic devices are likely to contain evidence of the commission of the Subject Offenses, such as spreadsheets or other financial documents or ledgers; emails with co-conspirators; notes of financial transactions; and/or web history or search history relating to the value of certain financial assets or other topics relevant to the commission of the Subject Offenses.

e. Based on my training and experience, Ellison's electronic devices are likely to contain location information that may be evidence that certain subjects of the investigation were located in the same place at a relevant period in time. Such location information may include

cellphone location data, IP records, photographs of locations, and/or calendar entries, and may establish that, for instance, two members of the conspiracy were together at, around, or shortly before the time they took an act in furtherance of the conspiracy.

f. Based on my training and experience, I have learned that individuals involved in cryptocurrency businesses often keep particular electronic devices, such as keys or ledgers, for use in tracing, encrypting or tracking cryptocurrency.

g. In addition, based on my training and experience, I have learned that individuals engaged in criminal activity often store such records, sometimes for years, as records of past relationships with co-conspirators, to keep track of co-conspirator's contact information, to keep a record of transactions, to store passwords or account information or accounts or devices used in furtherance of the criminal activity, or notes to follow up on other aspects of the scheme.

Search of Devices for Evidence of the Subject Offenses

14. Based on the foregoing, there is probable cause to believe that any electronic devices in the possession of Caroline Ellison or in the Subject Premises belonging to Ellison (collectively, the "Subject Devices"), contain evidence, fruits, and instrumentalities of the Subject Offenses. In particular, I believe the Subject Devices are likely to contain the following information:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses consisting of registration information, access logs, device information, user photographs, contact information, payment information, and other personally identifiable information.

b. Evidence concerning the relationship between FTX and Alameda, including the pooling of funds and the sharing of non-public information.

c. Evidence of statements, representations, and omissions made by Sam Bankman-Fried, Caroline Ellison, Alameda Research, FTX, or any of their agents or employees to customers, investors, or lenders concerning Alameda's and/or FTX's balance sheets, available assets, liquidity, and the use of customer funds.

d. Evidence of the financial condition of Alameda and FTX, including balance sheets, ledgers, financial statements, bank account records, profit and loss statements, audited financials, and financial working papers.

e. Evidence of loans to Alameda, the use of FTT as collateral on loans, and requests for the repayment of loans by Alameda.

f. Evidence concerning the financial condition of Alameda including any credit crunch, liquidity crisis, loan repayment or recapitalization demand, or financial loss to Alameda.

g. Evidence concerning Alameda's trading strategies and the use of leverage.

h. Evidence of the misuse of FTX's funds including but not limited to the transfer of FTX customer funds to Alameda, as well as agreements to do the same.

i. Evidence of knowledge by any Alameda or FTX employee of the misuse of FTX funds, including the transfer of FTX customer funds to Alameda.

j. Evidence concerning FTX's liabilities and knowledge of the same.

k. Evidence concerning the November 2, 2022, Coindesk.com article about Alameda's balance sheet.

l. Evidence concerning customer withdrawals from FTX on or after November 2, 2022, including but not limited to efforts to stop or slow customer withdrawals.

m. Evidence concerning attempts to generate funds or liquidity for FTX or Alameda on or after November 2, 2022.

n. Evidence concerning tweets made by Bankman-Fried or Ellison between November 2, 2022, and the date of this warrant.

o. Evidence of deletion of tweets, other electronic files, destruction of evidence, or attempts to obstruct justice.

p. Evidence of concealment of the misuse of FTX's funds including but not limited to the use of computer programs or software to conceal missing funds or the misappropriation of funds.

q. Evidence establishing the relationship between Ellison and co-conspirators.

r. Evidence of the geographic location of Ellison.

s. Evidence of passwords or other information needed to access the Subject Devices.

t. Evidence relating to other accounts, devices, or physical premises in which evidence of the commission of the Subject Offenses may be found.

u. Evidence that may aid law enforcement in identifying and accessing assets that may represent proceeds of fraud or are traceable to such proceeds of the Subject Offenses, such as login names, passwords, and private keys.

15. Based on my training and experience, I also know that, where electronic devices are used in furtherance of criminal activity, such as the Subject Devices, evidence of the criminal activity can often be found months or even years after it occurred. This is typically true because:

a. Electronic files can be stored on an electronic drive for years at little or no cost and users thus have little incentive to delete data that may be useful to consult in the future.

b. Even when a user does choose to delete data, the data can often be recovered months or years later with the appropriate forensic tools. When a file is "deleted" on an electronic device, the data contained in the file does not actually disappear, but instead remains, in "slack space,"

until it is overwritten by new data that cannot be stored elsewhere on the device. Similarly, files that have been viewed on the Internet are generally downloaded into a temporary Internet directory or "cache," which is only overwritten as the "cache" fills up and is replaced with more recently viewed Internet pages. Thus, the ability to retrieve from an electronic device depends less on when the file was created or viewed than on a particular user's operating system, storage capacity, and user habits.

c. In the event that a user changes electronic devices, the user will typically transfer files from the old device to the new device, so as not to lose data. In addition, users often keep backups of their data on electronic storage media such as thumb drives, flash memory cards, or portable hard drives.

16. As set forth above and in Attachment B, certain categories of materials to be searched, to the extent they are dated, will be limited to those sent, received, created, edited, or delated on or after January 1, 2021. While it appears that the misuse of funds occurred in or around 2022, evidence from 2021 is relevant to establish the financial condition of FTX and Alameda, the relationships between co-conspirators, and the background concerning certain financial transactions.

17. In addition to there being probable cause to believe that the Subject Devices contain evidence of the Subject Offenses, there is also probable cause to believe that the Subject Devices constitute instrumentalities of the Subject Offenses, because they were used to communicate with co-conspirators in furtherance of the Subject Offenses.

PROCEDURES FOR SEARCHING THE SUBJECT DEVICES

Unlocking Devices

18. I request authority to allow law enforcement agents to obtain from Caroline Ellison (but not any other individuals present at the Subject Premises at the time of execution of the warrants) the compelled display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s) requiring such biometric access subject to seizure pursuant to this warrant for which law enforcement has reasonable suspicion that the physical biometric characteristics of Ellison will unlock the device(s). This authority is not to compel Ellison to provide a numeric passcode, although she may be asked to voluntarily provide one. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home"

button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers (such as Apple's "Face ID") have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's

contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed above, there is reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device via Touch ID, and it is also possible that

the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device.

19. Due to the foregoing, I respectfully request that the Court authorize that, if law enforcement personnel encounter any device(s) that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, law enforcement personnel may obtain from Caroline Ellison the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any device(s), including to (1) press or swipe the fingers (including thumbs) of Ellison to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of Ellison to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Ellison to activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by the proposed warrants.

Execution of the Warrant for ESI

20. Federal Rule of Criminal Procedure 41(e)(2)(B) provides that a warrant to search for and seize property "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information . . . for later review." Consistent with Rule 41, this application requests authorization to seize any computer devices and storage media and transport them to an appropriate law enforcement facility for review. This is typically necessary for a number of reasons:

a. First, the volume of data on computer devices and storage media is often impractical for law enforcement personnel to review in its entirety at the search location.

b. Second, because computer data is particularly vulnerable to inadvertent or intentional modification or destruction, computer devices are ideally examined in a controlled environment, such as a law enforcement laboratory, where trained personnel, using specialized software, can make a forensic copy of the storage media that can be subsequently reviewed in a manner that does not change the underlying data.

c. Third, there are so many types of computer hardware and software in use today that it can be impossible to bring to the search site all of the necessary technical manuals and specialized personnel and equipment potentially required to safely access the underlying computer data.

d. Fourth, many factors can complicate and prolong recovery of data from a computer device, including the increasingly common use of passwords, encryption, or other features or configurations designed to protect or conceal data on the computer, which often take considerable time and resources for forensic personnel to detect and resolve.

Review of ESI

21. Following seizure of any computer devices and storage media and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will review the ESI contained therein for information responsive to the warrant.

22. In conducting this review, law enforcement personnel may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

a. surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

b. conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);

c. "scanning" storage areas to discover and possibly recover recently deleted data or deliberately hidden files; and

d. performing electronic keyword searches through all electronic storage areas to determine the existence and location of data potentially related to the subject matter of the investigation;[3] and

e. reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

23. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement personnel may need to conduct a complete review of all the ESI from seized devices or storage media to evaluate its contents and to locate all data responsive to the warrant.

[3] Keyword searches alone are typically inadequate to detect all relevant data. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.

Return of Devices

24. If the Government determines that the electronic devices are no longer necessary to retrieve and preserve the data, and the devices themselves are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return these items, upon request. Computer data that is encrypted or unreadable will not be returned unless law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

CONCLUSION

25. Based on the foregoing, I respectfully request the court to issue warrants to seize the items and information specified in Attachments A and B to this affidavit and to the search and seizure warrants.

/s/ Kristin Allain
Kristin Allain
Special Agent
Federal Bureau of Investigation

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3) and affirmed under oath the contents of this affidavit and application.

Date: November 16, 2022

Time: 10:38 AM, Nov 16, 2022

Hon. Andrea K. Johnstone
United States Magistrate Judge

ATTACHMENT A-1

The premises to be searched (the "Subject Premises") are described as follows, and include all locked and closed containers found therein: a single family home located at 360 Narrows Road, Barnstead, New Hampshire 03225.

Law enforcement agents are authorized to seize any and all cellphones, tablets, computers, electronic storage media, or other electronic devices belonging to Caroline Ellison (the "Subject Devices") within the Subject Premises. In lieu of seizing any Subject Device, this warrant also authorizes the copying of such devices or media for later review.

Included within the items to be seized from the Subject Premises are:

(i) Any items or records needed to access the data stored on any seized or copied computer devices or storage media, including but not limited to any physical keys, encryption devices, or records of login credentials, passwords, private encryption keys, or similar information.

(ii) Any items or records that may facilitate a forensic examination of the computer devices or storage media, including any hardware or software manuals or other information concerning the configuration of the seized or copied computer devices or storage media.

(iii) Any evidence concerning the identities or locations of those persons with access to, control over, or ownership of the seized or copied computer devices or storage media.

During the execution of the warrant, law enforcement personnel are authorized to obtain from Caroline Ellison the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Subject Devices, including to (1) press or swipe the fingers (including thumbs) of Ellison to the fingerprint scanner of the device(s); (2) hold the device(s) in front of the face of Ellison to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Ellison to activate the iris

recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

ATTACHMENT A-2

The person to be searched is Caroline Ellison who is depicted in the photograph below:

This warrant authorizes the search of Caroline Ellison's person and his personal effects in the immediate vicinity and control of Ellison at the location where the search warrant is executed, including any backpacks, briefcases, purses, and bags. The warrant authorizes the search, seizure, and forensic examination of any and all cellphones, tablets, computers, electronic storage media, and any other electronic devices on Ellison's person (collectively, the "Subject Devices"). In lieu of seizing any Subject Device, this warrant also authorizes the copying of such devices or media for later review.

During the execution of the warrant, law enforcement personnel are authorized to obtain from Ellison the display of any physical biometric characteristics (such as fingerprint/thumbprint or facial characteristics) necessary to unlock any Subject Devices, including to (1) press or swipe the fingers (including thumbs) of Ellison to the fingerprint scanner of the device(s); (2) hold the

device(s) in front of the face of Ellison to activate the facial recognition feature; and/or (3) hold the device(s) in front of the face of Ellison to activate the iris recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

ATTACHMENT B

Following seizure of any Subject Devices and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

The items to be seized from the Subject Devices consist of the following evidence, fruits, and instrumentalities of violations 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1349 (wire fraud conspiracy); and 18 U.S.C. §§ 1956 and 1957 (money laundering and money spending) (the "Subject Offenses") described as follows:

a. Evidence sufficient to establish the user(s) of the Subject Devices at times relevant to the Subject Offenses consisting of registration information, access logs, device information, user photographs, contact information, payment information, and other personally identifiable information.

b. Evidence concerning the relationship between FTX and Alameda, including the pooling of funds and the sharing of non-public information.

c. Evidence of statements, representations, and omissions made by Sam Bankman-Fried, Caroline Ellison, Alameda Research, FTX, or any of their agents or employees to customers, investors, or lenders concerning Alameda's and/or FTX's balance sheets, available assets, liquidity, and the use of customer funds.

d. Evidence of the financial condition of Alameda and FTX, including balance sheets, ledgers, financial statements, bank account records, profit and loss statements, audited financials, and financial working papers.

e. Evidence of loans to Alameda, the use of FTT as collateral on loans, and requests for the repayment of loans by Alameda.

f. Evidence concerning the financial condition of Alameda including any credit crunch, liquidity crisis, loan repayment or recapitalization demand, or financial loss to Alameda.

g. Evidence concerning Alameda's trading strategies and the use of leverage.

h. Evidence of the misuse of FTX's funds including but not limited to the transfer of FTX customer funds to Alameda, as well as agreements to do the same.

i. Evidence of knowledge by any Alameda or FTX employee of the misuse of FTX funds, including the transfer of FTX customer funds to Alameda.

j. Evidence concerning FTX's liabilities and knowledge of the same.

k. Evidence concerning the November 2, 2022, Coindesk.com article about Alameda's balance sheet.

l. Evidence concerning customer withdrawals from FTX on or after November 2, 2022, including but not limited to efforts to stop or slow customer withdrawals.

m. Evidence concerning attempts to generate funds or liquidity for FTX or Alameda on or after November 2, 2022.

n. Evidence concerning tweets made by Bankman-Fried or Ellison between November 2, 2022, and the date of this warrant.

o. Evidence of deletion of tweets, other electronic files, destruction of evidence, or attempts to obstruct justice.

p. Evidence of concealment of the misuse of FTX's funds including but not limited to the use of computer programs or software to conceal missing funds or the misappropriation of funds.

q. Evidence establishing the relationship between Ellison and co-conspirators.

r. Evidence of the geographic location of Ellison.

s. Evidence of passwords or other information needed to access the Subject Devices.

t. Evidence relating to other accounts, devices, or physical premises in which evidence of the commission of the Subject Offenses may be found.

u. Evidence that may aid law enforcement in identifying and accessing assets that may represent proceeds of fraud or are traceable to such proceeds of the Subject Offenses, such as login names, passwords, and private keys.

The materials seized pursuant to this warrant, if dated, are limited to those sent, received, created, edited, or delated on or after January 1, 2021.

Review of ESI

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;
- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and
- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the computer was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in this

Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.